

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-081969

(43)Date of publication of application : 21.03.2000

(51)Int.Cl.

G06F 7/58

(21)Application number : 10-267415

(71)Applicant : KUROSAWA KAORU  
TOYO COMMUN EQUIP CO LTD

(22)Date of filing : 04.09.1998

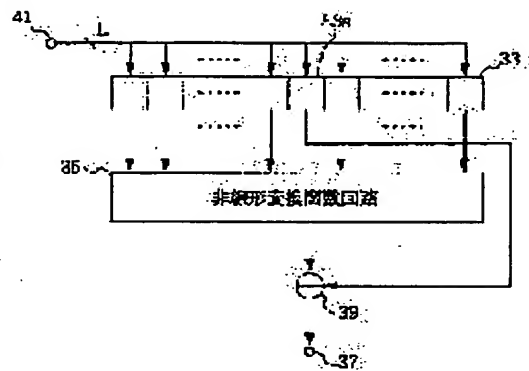
(72)Inventor : KUROSAWA KAORU  
SUGIMOTO KOICHI

## (54) PSEUDO-RANDOM NUMBER GENERATOR

## (57)Abstract:

PROBLEM TO BE SOLVED: To obtain good random number characteristics by assuring equal frequency characteristics of output by performing an exclusive OR operation between at least one register value of a linear feedback shift register and a nonlinear transformation value of the remaining register values.

SOLUTION: A nonlinear transformation function circuit 35 is connected with the linear feedback shift register 33 with L stages to generate an (m) system. In addition, an exclusive OR operation circuit 39 is connected between the nonlinear transformation function circuit 35 and an output terminal 37. Output of at least one stage 33a of the linear feedback shift register 33 with L stages is connected with the other input of the exclusive OR operation circuit 39. Since the linear feedback shift register 33 has a cycle of  $2L-1$ , when L is sufficiently large, kinds of appearance probability of 1, 0 of output in a nonlinear filter generator with this structure are regarded as equal. Therefore, the pseudo-random number generator with good random number characteristics in which kinds of appearance of 1, 0 are in equal frequency is obtained.



## LEGAL STATUS

[Date of request for examination] 27.09.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3533956

[Date of registration] 19.03.2004

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C): 1998,2003 Japan Patent Office

BEST AVAILABLE COPY

**THIS PAGE BLANK (USPTO)**

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-81969

(P2000-81969A)

(43) 公開日 平成12年3月21日 (2000.3.21)

(51) Int.Cl.<sup>7</sup>

G 0 6 F 7/58

識別記号

F I

G 0 6 F 7/58

テマコード (参考)

C

審査請求 未請求 請求項の数 2 F D (全 8 頁)

(21) 出願番号 特願平10-267415

(22) 出願日 平成10年9月4日 (1998.9.4)

特許法第30条第1項適用申請有り 1998年3月6日 社団法人電子情報通信学会発行の「1998年電子情報通信学会総合大会講演論文集基礎・境界」に発表

(71) 出願人 598129163

黒澤 馨

神奈川県川崎市高津区諏訪2-7-3 パステルハイツ205

(71) 出願人 000003104

東洋通信機株式会社

神奈川県高座郡寒川町小谷2丁目1番1号

(72) 発明者 黒澤 馨

神奈川県川崎市高津区諏訪2-7-3 パステルハイツ205

(74) 代理人 100085660

弁理士 鈴木 均

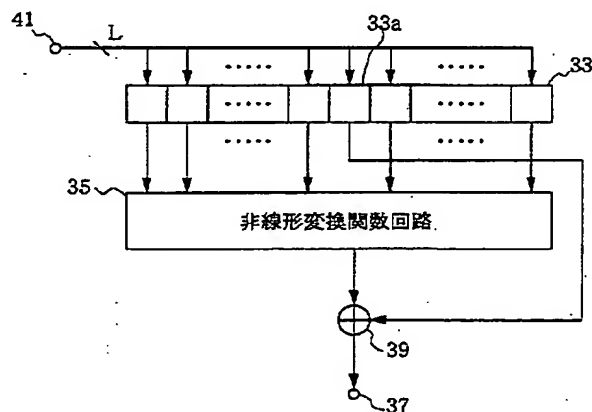
最終頁に続く

(54) 【発明の名称】 擬似乱数発生装置

(57) 【要約】

【課題】 出力の1、0の等頻度性を保障して良好な乱数特性を得ることができる擬似乱数発生装置を提供する。

【解決手段】 暗号通信装置などで使用される擬似乱数を発生させる擬似乱数発生装置であって、クロックに同期して動作するm系列を生成する線形フィードバックシフトレジスタと、上記線形フィードバックシフトレジスタの各レジスタ値を非線形変換して1ビットの出力を得る非線形変換関数手段と、上記線形フィードバックシフトレジスタに初期値を設定する初期値設定手段と、上記線形フィードバックシフトレジスタ内少なくとも1つの線形フィードバックシフトレジスタのレジスタ値を残りの線形フィードバックシフトレジスタのレジスタ値の非線形変換値と排他的論理和演算を施して擬似乱数として出力する排他的論理和演算手段とを具備する構成となっている。



## 【特許請求の範囲】

【請求項1】 暗号通信装置などで使用される擬似乱数を発生させる擬似乱数発生装置であって、クロックに同期して動作するm系列を生成する線形フィードバックシフトレジスタと、

上記線形フィードバックシフトレジスタの各レジスタ値を非線形変換して1ビットの出力を得る非線形変換関数手段と、

上記線形フィードバックシフトレジスタに初期値を設定する初期値設定手段と、

上記線形フィードバックシフトレジスタ内少なくとも1つの線形フィードバックシフトレジスタのレジスタ値を残りの線形フィードバックシフトレジスタのレジスタ値の非線形変換値と排他的論理和演算を施して擬似乱数として出力する排他的論理和演算手段とを具備することを特徴とする擬似乱数発生装置。

【請求項2】 暗号通信装置などで使用される擬似乱数を発生させる擬似乱数発生装置であって、クロックに同期して動作するm系列を生成する線形フィードバックシフトレジスタと、上記線形フィードバックシフトレジスタの各レジスタ値を線形変換し出力する線形変換手段と、上記線形変換値を非線形変換して1ビットを出力する非線形変換手段と、上記線形フィードバックシフトレジスタに初期値を設定する初期値設定手段とを具備し、上記非線形変換手段は、上記線形変換手段の少なくとも1ビットの出力を残りの線形変換手段の非線形変換値と排他的論理和演算を行い擬似乱数として出力するものであって、上記線形変換手段は、線形フィードバックシフトレジスタの状態遷移行列のべきで表現できることを特徴とする擬似乱数発生装置。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、暗号通信装置などで使用される擬似乱数を発生させる擬似乱数発生装置に関し、特に、出力の1、0の等頻度性を保障して良好な乱数特性を得ることができる擬似乱数発生装置としてのフィルタジェネレータに関する。

## 【0002】

【従来の技術】従来より、電話、無線、データ通信などの通信システムにおいて、伝送情報が第三者に知られないようにするために、伝送情報を暗号化することが行われる。この暗号化方式で特に高速通信に利用されるものの中にストリーム暗号方式がある。ストリーム暗号方式は、擬似乱数発生装置の出力する擬似乱数を1ビット単位でデータストリームと排他的論理和演算を施すことでデータストリームの暗号化を行うものである。すなわ

ち、一般のストリーム暗号装置は、図4に示す様に、データストリームの入力端子1と出力端子3との間に排他的論理和演算回路5が接続され、上記排他的論理和演算回路5の他方の入力に擬似乱数発生装置7の出力が接続

されている。そして、上記擬似乱数発生装置7には入力端子9およびクロック入力端子11が接続され、初期値およびクロック信号が入力される。図5は従来の擬似乱数発生装置の一例であるノンリニアフィルタジェネレータ(Nonlinear Filter Generator)の構成図を示すものである。図5に示す様に、このノンリニアフィルタジェネレータは、入力端子13およびクロック入力端子15に接続された線形フィードバックシフトレジスタ17に非線形変換関数回路19が接続され、上記非線形変換関数回路19に出力端子21が接続されている。上記ノンリニアフィルタジェネレータは、クロック入力端子15よりのクロックに同期して動作する線形フィードバックシフトレジスタ17の各レジスタ値を入力とする非線形変換関数回路19の出力系列を擬似乱数系列としている。

【0003】図6に上記線形フィードバックシフトレジスタの一つであるスタンダード型線形フィードバックシフトレジスタの構成を示す。このスタンダード型線形フィードバックシフトレジスタは、図6に示す様に、複数(この場合L)のレジスタ23と複数(この場合L-1)の排他的論理和演算回路25とが直列に接続され、上記各レジスタ23の出力と各排他的論理和演算回路25の一方の入力との間にフィードバックタップ27が接続されている。上記線形フィードバックシフトレジスタの段数をLとすると、1つのレジスタに注目した時、出力系列の最大周期は $2^L - 1$ となることが知られており、この系列をm系列と呼ぶ。例えば、図6に示す線形フィードバックシフトレジスタにおいてm系列を生成するには、次のようにする。図6において、 $c_1, c_2, \dots, c_{L-1}$ はフィードバックタップと呼ばれ、タップが1のとき結線を示し、0のとき断線を示すものである。このとき線形フィードバックシフトレジスタの出力系列の特性多項式は、次のように表される。

## 【0004】

【数1】

$$C(X) = X^L + c_1 X^{L-1} + c_2 X^{L-2} + \dots + c_{L-1} X + 1 \quad (1)$$

上式が原始的な既約多項式となるようにすれば、線形フィードバックシフトレジスタはm系列を生成するようになる。図6に示す線形フィードバックシフトレジスタの

時刻 $t$ における状態を、

【0005】

【数2】

$$s(t) = (s_1(t), \dots, s_l(t))^T$$

と表すとき（ここで、 $T$ は転置を示す）、1クロック入力後の線形フィードバックシフトレジスタの状態を、

$$\begin{pmatrix} s_1(t+1) \\ s_{l-1}(t+1) \\ \vdots \\ s_3(t+1) \\ s_2(t+1) \\ s_1(t+1) \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & c_1 & c_2 & \cdots & c_{l-2} & c_{l-1} \end{pmatrix} \begin{pmatrix} s_1(t) \\ s_{l-1}(t) \\ \vdots \\ s_3(t) \\ s_2(t) \\ s_1(t) \end{pmatrix}$$

と表される。即ち、

【0008】

【数5】

$$s(t+1) = T_s s(t)$$

である。ここに、 $T_s$ は状態遷移行列である。従って、 $i$ クロック後の線形フィードバックシフトレジスタの状態は、状態遷移行列のべき $T_s^i$ を用いて、

【0009】

【数6】

$$s(t+i) = T_s^i s(t)$$

のように表される。上記線形フィードバックシフトレジスタの構成には他にモジュラー型、ハイブリッド型が存在する。これらは、Laung-Terng Wang, Edward J. Macc luskey著の論文、"Hybrid Designs Generating Maximum Length Sequences," IEEE Trans.on Computer-Aided Design, Vol.7, No.1, January, 1988等に示されている。

【0010】

【発明が解決しようとする課題】しかしながら、従来のノンリニアフィルタジェネレータ（Nonlinear Filter Generator）においては、線形フィードバックシフトレジスタの各レジスタ値が互いに独立ではないため、出力の1、0の等頻度性が保障されておらず乱数特性が悪かつ※

$$f(x_1, x_2, \dots, x_k) = g(x_1, \dots, x_{i-1}, x_{i+1}, x_k) + x_i \quad \cdots (2)$$

とすればよいことになる。ここで、 $x_i, f, g \in$

{0, 1}である。ところが上記コンビネーションジェネレータを用いたとき暗号の強度を高くしようとするとフィードバックレジスタを多数用意しなければならず、上記ノンリニアフィルタジェネレータに比べてハード構成が大きくなるという欠点があった。本発明は、上記事情に鑑みてなされたものであって、出力の1、0の等頻度性を保障して良好な乱数特性を得ることができる擬似乱数発生装置としてのフィルタジェネレータを提供することを目的とする。

※【0006】

※【数3】

$$s(t+1) = (s_1(t+1), \dots, s_l(t+1))^T$$

と表せば、状態遷移は、

【0007】

【数4】

※た。また、擬似乱数発生装置としてコンビネーションジェネレータ（Combination Generator）を用いれば、1の等頻度性を保障することができる。図7は、上記コンビネーションジェネレータの概略構成図である。図7に示す様に、上記コンビネーションジェネレータは、非線形変換関数回路29に各線形フィードバックシフトレジスタ31が接続されている構成となっており、各線形フィードバックシフトレジスタ31の周期の最大公約数が1である場合にそれぞれの線形フィードバックシフトレジスタ31の出力系列を独立とみなすことができる。さらに各線形フィードバックシフトレジスタ31の出力における1、0の等頻度性が保障されるならば、非線形変換関数回路29への入力はいったくランダムな系列とみなすことができる。1、0の出現頻度が如何に偏った系列であってもランダムな系列とビット毎に排他的論理和演算を施した系列はランダムな系列となる。したがって、上記コンビネーションジェネレータにおいて、1、0が等頻度となるような非線形変換関数回路29は、少なくとも1つの入力を残りの入力の非線形変換値と排他的論理和演算を施す構成とすればよい。すなわち、非線形変換関数は、

【0011】

【数7】

【0012】

【課題を解決するための手段】上記目的を達成するため、本発明は、暗号通信装置などで使用される擬似乱数発生させる擬似乱数発生装置において、クロックに同期して動作する $m$ 系列を生成する線形フィードバックシフトレジスタと、上記線形フィードバックシフトレジスタの各レジスタ値を非線形変換して1ビットの出力を得る非線形変換関数手段と、上記線形フィードバックシフトレジスタに初期値を設定する初期値設定手段と、上記線形フィードバックシフトレジスタ内少なくとも1つの

線形フィードバックシフトレジスタのレジスタ値を残りの線形フィードバックシフトレジスタのレジスタ値の非線形変換値と排他的論理和演算を施して擬似乱数として出力する排他的論理和演算手段とを具備することを特徴とする。本発明の他の特徴は、暗号通信装置などで使用される擬似乱数を発生させる擬似乱数発生装置において、クロックに同期して動作するm系列を生成する線形フィードバックシフトレジスタと、上記線形フィードバックシフトレジスタの各レジスタ値を線形変換し出力する線形変換手段と、上記線形変換値を非線形変換して1ビットを出力する非線形変換手段と、上記線形フィードバックシフトレジスタに初期値を設定する初期値設定手段とを具備し、上記非線形変換手段は、上記線形変換手段の少なくとも1ビットの出力を残りの線形変換手段の非線形変換値と排他的論理和演算を行い擬似乱数として出力するものであって、上記線形変換手段は、線形フィードバックシフトレジスタの状態遷移行列のべきで表現できることである。

【0013】

【発明の実施の形態】以下、本発明を図示した実施形態に基づいて説明する。図1は、本発明による擬似乱数発生装置としてのノンリニアフィルタジェネレータの一実施形態を示す構成図である。図1に示す様に、このノンリニアフィルタジェネレータは、m系列を生成するL段の線形フィードバックシフトレジスタ33と、上記線形フィードバックシフトレジスタ33に接続された非線形変換関数回路35と、上記非線形変換関数回路35と出力端子37との間に接続された排他的論理和演算回路3\*

$$f(x_1, \dots, x_n) = g(x_1, \dots, x_{m-1}, x_{m+1}, x_n) \oplus x_m \quad \dots(3)$$

と表現できる。ここで、 $x_i = s_{a_i}$ 、 $(1 \leq i \leq n)$  ただし、 $1 \leq a_1 < a_2 < \dots < a_n \leq L$  である。また、 $f, g \in \{0, 1\}$  である。上記線形フィードバックシフトレジスタ33の1周期においては、非線形関数への入力 $(x_1, \dots, x_n)$ は、 $(0, \dots, 0)$ 以外の各種を $2^{L-n}$ 回ずつ、 $(0, \dots, 0)$ を $2^{L-n} - 1$ 回とることがわかる。もし、 $(x_1, \dots, x_n)$ において各種の出現確率が同じであるならば、ノンリニアフィルタジェネレータの出力の1、0の出現確率は等しい。これは、 $(x_1, \dots, x_n)$ において各種の出現確率が同じであるならば、 $g$ への入力 $(x_1, \dots, x_{m-1}, x_{m+1}, x_n)$ がある特定値であるとき、 $x_m$ は1、0を等頻度でとるからである。しかし、実際は、 $(x_1, \dots, x_n)$ において $(0, \dots, 0)$ をとる場合が他の値をとる場合より1回少ない。従って、 $f(0, \dots, 0)$ の値が1回分少なくなる。以上から、 $z_0 = f(0, \dots, 0)$ とすれば、線形フィードバックシフトレジスタの1周期において、出力が $z_0$ となるのは $2^{L-n} - 1$ 回であり、出力が

【数9】

\*9とを有しており、上記排他的論理和演算回路39のもう一方の入力には、上記L段の線形フィードバックシフトレジスタ33の少なくとも1段33aの出力が接続されている。また、上記L段の線形フィードバックシフトレジスタ33には初期値入力のための入力端子41が接続されている。次に、上記ノンリニアフィルタジェネレータの動作について説明する。

【0014】上記入力端子41より初期値が設定されシフト動作する上記L段の線形フィードバックシフトレジスタ33の所定の1段のレジスタ33aを除くレジスタよりの各レジスタ値が、上記非線形変換関数回路35へ入力され非線形変換される。そして、上記非線形変換関数回路35よりの非線形変換値に対し、上記所定の1段のレジスタ33aよりのレジスタ値を上記排他的論理和演算回路39によって排他的論理和演算し擬似乱数系列として上記出力端子37より出力する。次に、上記構成動作のノンリニアフィルタジェネレータの出力における1、0の等頻度性について説明する。上記L段の線形フィードバックシフトレジスタ33の各レジスタ値を $s_1, s_2, \dots, s_L$ とし、m系列を発生するものとする。ただし、 $s_i \in \{0, 1\}$ とする。すると、この線形フィードバックシフトレジスタ33は $2^L - 1$ なる周期を持つから、その1周期において $(s_1, s_2, \dots, s_L) \neq (0, 0, \dots, 0)$ 以外の全ての状態を1回ずつとる。また、非線形関数は、

【0015】

【数8】

$$z_0 \oplus 1$$

となるのは $2^{L-n}$ 回である。Lが十分に大きければ、上記ノンリニアフィルタジェネレータにおける出力の1、0の出現確率は等しいとみてよいこととなる。次に、上記図1に示したノンリニアフィルタジェネレータの具体例について説明する。図2は、上記図1に示したノンリニアフィルタジェネレータの具体例の構成図である。図2に示す様に、このノンリニアフィルタジェネレータは、線形フィードバックシフトレジスタ43が、4段のD型フリップフロップ45～51と、4段目のD型フリップフロップ51の出力と1段目のD型フリップフロップ45の出力との排他的論理和演算を行って上記1段目のD型フリップフロップ45へ出力する第1の排他的論理和回路53とを有しており、上記各D型フリップフロップ45～51には初期値設定用の入力端子55およびクロック信号入力用のクロック端子57が接続されている。そして、このノンリニアフィルタジェネレータの非線形変換関数回路59が、上記1段目のD型フリップフロップ45に設定されている値と上記4段目のD型フリップフロップ51に設定されている値との論理積演算を

施すための論理積演算回路61を有しており、上記論理積演算回路61の出力と上記2段目のD型フリップフロップ47の出力との排他的論理和演算が第2の排他的論理和演算回路63によって施され出力端子65より出力される。

【0016】次に、上記ノンリニアフィルタジェネレータの動作について説明する。まず、上記線形フィードバックシフトレジスタ43内のD型フリップフロップ45～51に上記入力端子55を通して初期値が設定される。上記クロック端子57よりクロック入力があると、上記D型フリップフロップ47～51にはそれぞれD型フリップフロップ45～49に記憶されていた値が設定され、上記1段目のD型フリップフロップ45には上記1段目のD型フリップフロップ45に記憶されていた値と上記4段目のD型フリップフロップ51に記憶されていた値の排他的論理和値が設定される。上記非線形変換関数回路59（論理積演算回路61）は線形フィードバックシフトレジスタ43の各レジスタの出力のうち上記1段目のD型フリップフロップ45および4段目のD型フリップフロップ51に設定されている値の論理積値を出力し、上記論理積値と上記2段目のD型フリップフロップ47に設定されている値の排他的論理和演算を施した値が出力端子65より出力される。従って、初期値として上記D型フリップフロップ45～51の全てに1を設定したとすると、上記出力端子65に現れる出力系列は、0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1の繰り返しとなり、1, 0の出現確率は等しいとみてよいことがわかる。

【0017】次に、上記図2に示した具体例の変形例について図3を参照して説明する。図3に示したノンリニアフィルタジェネレータは、図2に示したものと等価となっている。すなわち、図3に示す様に、このノンリニアフィルタジェネレータは、線形フィードバックシフトレジスタ67が、4段のD型フリップフロップ69～75と、4段目のD型フリップフロップ75の出力と1段目のD型フリップフロップ69の出力との排他的論理和演算を行って上記1段目のD型フリップフロップ69へ出力する第1の排他的論理和回路77とを有しており、上記各D型フリップフロップ69～75には初期値設定用の入力端子79およびクロック信号入力用のクロック端子81が接続されている。そして、このノンリニアフィルタジェネレータの非線形変換関数回路83が、上記1段目のD型フリップフロップ69に設定されている値と上記4段目のD型フリップフロップ75に設定されている値との排他的論理和演算を施す第2の排他的論理和演算回路85と、上記3段目のD型フリップフロップ73に設定されている値と上記第2の排他的論理和演算回路85の出力との論理積演算を施すための論理積演算回路87とを有しており、上記論理積演算回路87の出力と上記1段目のD型フリップフロップ69の出力との排

他的論理和演算が第3の排他的論理和演算回路89によって施され出力端子91より出力される。従って、初期値として上記D型フリップフロップ69～75の全てに1を設定したとすると、上記出力端子91に現れる出力系列は、1, 1, 1, 0, 0, 1, 0; 1, 1, 0, 0, 0, 1, 1, 0の繰り返しとなり、これは図2に示したノンリニアフィルタジェネレータの出力端子65に現れる系列が1クロックだけ遅れた系列であるため、同じ系列である。

【0018】以下に図3に示したノンリニアフィルタジェネレータが図2に示したノンリニアフィルタジェネレータを等価変換することによって作られたものであることを示す。図2において時刻tにおける1段目のD型フリップフロップ45のレジスタ値をs(t)で表す。すると、2段目のD型フリップフロップ47はs(t-1)となり、3段目のD型フリップフロップ49、4段目のD型フリップフロップ51はそれぞれ、s(t-2), s(t-3)と表される。従って、出力端子65に現れる時刻tにおける出力は、

【0019】

【数10】

$$s(t)s(t-3) \oplus s(t-1) \quad \cdots (4)$$

となる。ここで、線形フィードバックシフトレジスタ43の構造から、

【0020】

【数11】

$$s(t) = s(t-1) \oplus s(t-4) \quad \cdots (5)$$

なる関係が成り立つ。同様に、図3において時刻tにおける上記1段目のD型フリップフロップ69のレジスタ値を

【0021】

【数12】

$$\bar{s}(t)$$

で表すると、出力端子91に現れる時刻tにおける出力は、

【0022】

【数13】

$$(\bar{s}(t) \oplus \bar{s}(t-3))\bar{s}(t-2) \oplus \bar{s}(t) \quad \cdots (6)$$

となり、上記線形フィードバックシフトレジスタ67の構造から、

【0023】

【数14】

$$\bar{s}(t) = \bar{s}(t-1) \oplus \bar{s}(t-4) \quad \cdots (7)$$

が成り立つ。上記出力端子91に現れる出力が上記出力端子65に現れる出力に対して1クロック遅れているから、s(t)と

【0024】  
【数15】

$$\bar{s}(t)$$

の間には、

【0025】  
【数16】

$$\bar{s}(t) = s(t-1)$$

なる関係がある。これを上記式(6)に代入すれば、

【0026】  
【数17】

$$(s(t-1) \oplus s(t-4))s(t-3) \oplus s(t-1) \quad \cdots (8)$$

を得る。また、上記式(7)の関係と

【0027】  
【数18】

$$\bar{s}(t) = s(t-1)$$

を組み合わせると上記(8)式に代入すれば、上記(4)式を得ることができる。従って、上記図3のノンリニアフィルタジェネレータが図2のノンリニアフィルタジェネレータを等価変換することによって作られたものであることがわかる。上記の変形実施例を含めて本発明を一般化して表現すると図8のようになる。同図において、図1と同じ構成には同じ符号を付した。図8が図1と異なる点は、線形フィードバックシフトレジスタ33と非線形変換回路35との間に、線形フィードバックシフトレジスタ33の状態遷移行列 $T_s$ 、のべき $T_s^{-1}$ で表される線形変換回路100を配置したところにある。先に述べたように図8における線形フィードバックシフトレジスタ33の状態遷移行列 $T_s$ 、のべき $T_s^{-1}$ で表される線形変換回路100の出力は、線形フィードバックシフトレジスタ33の状態出力を*i*クロック分時間シフトしたものであるから、図1に示されるノンリニアフィルタジェネレータと同様に、図8に示されるノンリニアフィルタジェネレータの出力における1、0の出現確率も等しいとみてよいこととなる。例えば、図3の構成を図8に基づいて表現すると図9のようになる。同図において101が線形変換回路である。このときの線形フィードバックシフトレジスタ67の状態遷移行列 $T_s$ は、

【0028】  
【数19】

$$T_s = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

であり、線形変換回路101は $T_s$ 、のべきとなる。この例では $T_s^{-1} = T_s$ 、となる。線形フィードバックシフトレジスタ67の状態を、

【0029】  
【数20】

$$s(t) = (s_4(t), s_3(t), s_2(t), s_1(t))^T$$

と表し、線形変換回路101の出力を

【0030】  
【数21】

$$u(t) = (u_4(t), u_3(t), u_2(t), u_1(t))^T$$

と表せば、

【0031】  
10 【数22】

$$u(t) = T_s s(t)$$

すなわち、

【0032】  
【数23】

$$\begin{pmatrix} u_4(t) \\ u_3(t) \\ u_2(t) \\ u_1(t) \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} s_4(t) \\ s_3(t) \\ s_2(t) \\ s_1(t) \end{pmatrix}$$

と表せるので、これより、

【0033】  
【数24】

$$u_1(t) = s_1(t) \oplus s_4(t),$$

$$u_2(t) = s_1(t),$$

$$u_3(t) = s_2(t),$$

$$u_4(t) = s_3(t)$$

を得る。従って、図3の場合は線形変換回路が図9のように表されることになる。

【0034】

【発明の効果】本発明は、以上説明したように、クロック入力に同期して動作する線形フィードバックシフトレジスタの各レジスタ値を非線形変換関数回路に入力し、クロック毎に擬似乱数を出力する構成において上記線形フィードバックシフトレジスタの少なくとも1つのレジスタ値を残りのいくつかのレジスタの非線形変換値と排他的論理和演算を施す様にしている、或いは、線形フィードバックシフトレジスタの各レジスタ値を線形変換回路に入力し、その出力である線形変換値を非線形変換回路に入力したものにあっては、線形変換出力の少なくとも1ビットの出力を残りのいくつかの線形変換出力の非線形変換値と排他的論理和演算を施すようにしてい

るので、1、0の出現が等頻度である乱数特性のよい擬似乱数発生装置が提供できる。

【図面の簡単な説明】

【図1】本発明による擬似乱数発生装置としてのノンリニアフィルタジェネレータの一実施形態を示す構成図である。

【図2】上記図1に示したノンリニアフィルタジェネレータの具体例の構成図である。

【図3】図2に示したノンリニアフィルタジェネレータの変形例の構成図である。

【図4】一般のストリーム暗号装置の構成図である。

【図5】従来の擬似乱数発生装置の一例であるノンリニアフィルタジェネレータの構成図である。

【図6】一般のスタンダード型の線形フィードバックシフトレジスタの構成図である。

【図7】従来の擬似乱数発生装置の一例であるコンビネ\*

\*ーションジェネレータの構成図である。

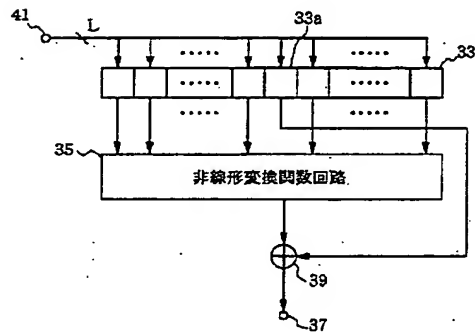
・【図8】本発明に係る説明図である。

【図9】本発明に係る説明図である。

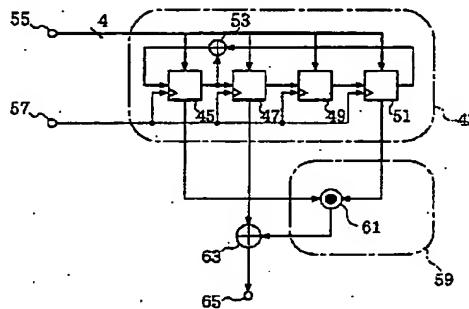
【符号の説明】

1…平文入力端子、3…暗号文出力端子、5、39、53、63、77、85、89…排他的論理和演算回路、7…擬似乱数発生装置、9、13、41、55、79…初期値設定用端子、11、15、57、81…クロック入力用端子、17、33、43、67…線形フィードバックシフトレジスタ、19、29、35、59、83…非線形変換関数回路、21、37、65、91…擬似乱数出力端子、23、45～51、69～75…D-FlipFlop素子、25…排他的論理和演算素子、31…線形フィードバックシフトレジスタ、61、87…論理積演算回路、

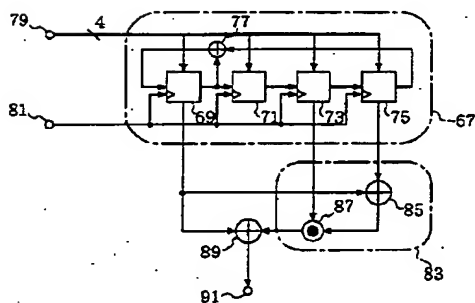
【図1】



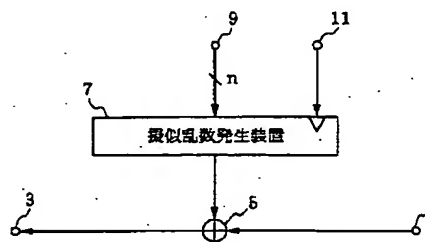
【図2】



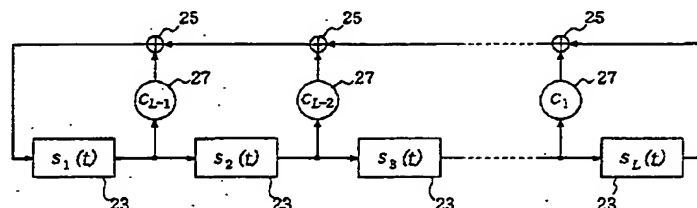
【図3】



【図4】



【図6】

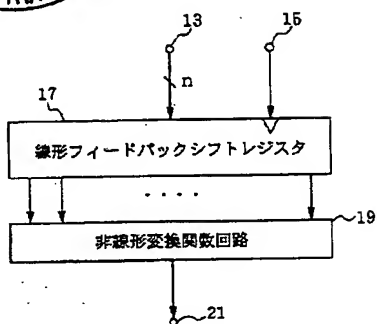




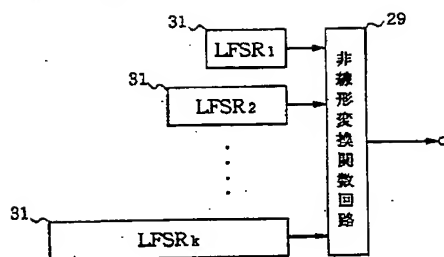
(8)

特開2000-81969

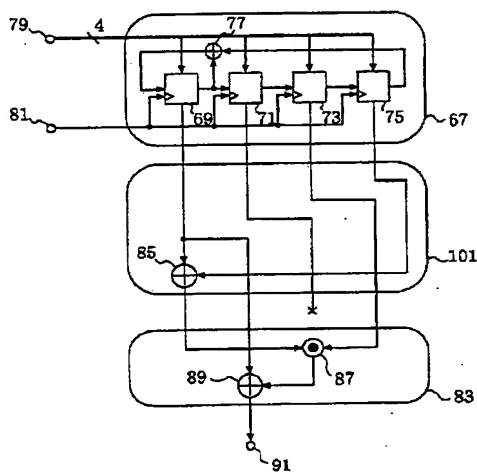
【図5】



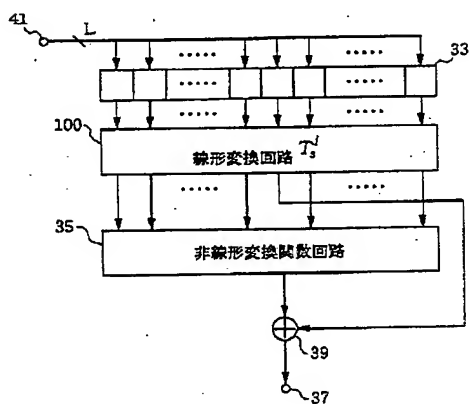
【図7】



【図9】



【図8】



フロントページの続き

(72)発明者 杉本 浩一  
神奈川県高座郡寒川町小谷二丁目1番1号  
東洋通信機株式会社内